IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
v.	)	Civil Action No.:
	)	2:18cv94
CISCO SYSTEMS, INC.,	)	
	)	
Defendant.	)	

TRANSCRIPT OF VIDEOCONFERENCE BENCH TRIAL PROCEEDINGS

Norfolk, Virginia
May 13, 2020

Volume 6B
Pages 827-897

BEFORE: THE HONORABLE HENRY C. MORGAN, JR.
United States District Judge

Appearances: (Via Zoomgov Video)

KRAMER LEVIN NAFTALIS & FRANKEL, LLP
By: JAMES RUSSELL HANNAH
PAUL JOSEPH ANDRE
Counsel for Plaintiff

DUANE MORRIS, LLP
By: MATTHEW GAUDET
LOUIS NORWOOD JAMESON
Counsel for Defendant

I N D E X

E X H I B I T S

P R O C E E D I N G S

(Proceedings resumed at 2:07 p.m. as follows:)

THE COURT: All right. Mr. Gaudet, let's pick up where we left off.

MR. GAUDET: Thank you, Your Honor.

CROSS-EXAMINATION (Cont'd.)

BY MR. GAUDET:

Q. Dr. Mitzenmacher, do you recall when we broke for lunch we were talking about the transactional-commit model that you're accusing in the firewalls, correct?

A. Yes.

Q. Okay. Now, I just want to establish what's new and what's old. So let's pull up Plaintiff's Exhibit 1196.

MR. GAUDET: And Your Honor, Plaintiff's Exhibit 1196 should be, actually it's in your small binder as well. It's in both. So the small binder for cross-examination should have it.

THE COURT: I have it.

MR. GAUDET: Okay.

BY MR. GAUDET:

Q. And Dr. Mitzenmacher, you see the front page of this? This is a document in the 2013, at least it began in 2013 to talk about the transactional-commit model. Do you see that in the title?

A. I see transactional-commit model in the title, and I see the first revision date of 9/12/2013.

MR. GAUDET: Mr. Simons, let's go to Page 7 of this document.

THE COURT: Has this been admitted?

COURTROOM DEPUTY CLERK: Yes.

MR. GAUDET: Your Honor, I believe PTX1196 was admitted in the plaintiff's case-in-chief.

THE COURT: Okay. Page 007.

MR. GAUDET: 007. I think I made a joke about that, Your Honor, and I drew no laughter.

Mr. Simons, let's highlight in the section right under 1 5, Proposal to Customer, first line, the phrase "We proposed a transactional-commit model for ASA rule engine. Okay? Keep on highlighting the behavior changes from the legacy model to the proposed new model are described below. Okay.

BY MR. GAUDET:

Q. Dr. Mitzenmacher, can you confirm, based on this, that the transactional-commit model you are accusing, that's the new model, and the legacy model referenced on this document, that's the old model, correct?

A. I believe so.

Q. Okay. Now I want to set this side-by-side with the document we were looking at last time, to bring this all together to be sure we're absolutely clear, on what's what.

So let's pull up --

THE COURT: I'm clear on that.

MR. GAUDET: Okay, terrific. Your Honor, one other housekeeping item, which is we want to move to admit DTX-1290. We discussed that just before lunch. It had this, essentially this same image with some slightly references.

THE COURT: DTX-1290 will be admitted.

(Exhibit DTX-1290 received in evidence.)

MR. GAUDET: Thank you, Your Honor.

If we can, Mr. Simons, pull up the '806 claim language chart.

BY MR. GAUDET:

Q. We're going to, Dr. Mitzenmacher, while we're getting that pulled up, we're going to shift gears just little bit and I want to focus on the issue of caching. And to orient, you see that beginning at about Element G there, beginning at Element G, I should say, there's a reference to "signaling each processor to process packets in accordance with the second rule set." Do you see that?

A. Yes.

Q. Okay. And when you signal the processor to process packets, it sets off a string of things, right?

A. Yes.

Q. Okay. One of those is H1, you have to cease processing packets, right?

A. Yes. With the understanding of the descriptions in the patent; that is, you may have to complete whatever is in flight and then you'll stop and wait for the next step.

Q. And you cache the one or more packets, right?

A. Yes. You cache the packets that you ceased processing.

Q. Then, then we reconfigure the device, reconfigure the device then, to process packets with the second rule set or the new rule set, right?

A. That looks like H3.

Q. Okay. And then when you're done with that reconfiguration, then you resume processing and you do that with the new rule set, is that fair?

A. Roughly speaking, sure.

Q. Okay. Now you're saying that this cache, that these -- let's -- and this caching is satisfied by something called the packet buffer, right?

A. Yes.

Q. Okay. Now, packet buffering, right, I mean that, you can't process any packets without a packet buffer; is that fair?

A. I'm not quite are clear on your question. I mean...

Q. This is my point. Okay. Packet buffering is a thing that happens as a matter of course any time you process a packet in any context; is that fair?

A. You may typically have a packet buffer, and that packet buffer is be used to hold packets for various reasons.

Certainly.

Q. And whether or not -- I'm sorry, were you complete, Dr. Mitzenmacher?

A. I mean, I'm just agreeing you can have a packet buffer. I guess I'm not quite clear what buffer we're talking about quite yet, but I imagine you'll clarify with your questions.

Q. Well, and I mean this generally: Whether or not you have ceased processing some packets, any time you're processing packets, there's going to be a packet buffer that's holding the packet you're working on and it's holding the next one in line?

A. I mean, the packet buffer I don't think, if I understand, you would be holding the packet you're working on. At that point it should be out of the buffer. If there are packets waiting there may be packets being held in a packet buffer that would be awaiting processing, including, for instance, in this situation.

BY MR. GAUDET:

Q. Okay. And let's pull up Plaintiff's Exhibit 1917. This was some deposition testimony you cited yesterday.

MR. GAUDET: Now Your Honor, this has already been admitted. This should be in the Plaintiff's -- well, I assume it's in the Plaintiff's binder. It's Plaintiff's Exhibit 1917.

THE COURT: Yes.

BY MR. GAUDET:

Q. And Dr. Mitzenmacher, you pointed to this testimony

identifying the fact that there was a packet buffer to support your argument that that must be a cache, right?

A. A packet buffer is a cache, yes.

Q. Okay. Now, there was testimony from this same witness on the previous page that spoke to the issue of packet buffers as well -- or actually let me -- I don't expect you to know that off the top of your head, so let me withdraw that question.

A. Okay.

Q. Let's just put up, let's put up DTX-1650. And you see the one PTX-1917 that's Page 26. Do you see that? So now this is that same witness, but the prior page. And moving on to your answer. So if -- I'll give everyone a moment to read that.

MR. GAUDET: Your Honor, let me know if you're ready to proceed.

THE COURT: Yes.

BY MR. GAUDET:

Q. Dr. Mitzenmacher, is your understanding consistent with Mr. Hughes, that all routers have packet buffers where the packets are stored before processing, that's the way that Cisco has done packet processing since its inception? For decades?

A. I mean, I think I can't speak for all routers or in particular for all Cisco routers. I recognize that packet buffers may appear for a variety of reasons in a variety of places.

Q. Okay. Now, the word cache, the word cache, that's a

well-known word, right?
A. Yes. Although -- yeah. Yes, it's a well-known word in computing.
Q. Okay. None of the documents you cited yesterday actually used the word cache, right? Talked about buffers?
A. I don't know. I can't recall. Again, a buffer is a typical way that you would -- or one of the ways you would implement the cache. They both refer to memory.
Q. But the mere fact that a product has a buffer -- let me strike that.
The mere fact that a router or a switch has a buffer doesn't tell you much by itself other than the fact that you've got a router or switch, because they have all have buffers: Is that fair? What do you mean all routers have buffers?
THE COURT: What he apparently means is that all Cisco routers have buffers.
MR. GAUDET: Absolutely. And I thought the witness actually expanded out a little bit beyond that, but Your Honor's point is very well taken.
BY MR. GAUDET:
Q. All it tells you is you've got a Cisco router or buffer since their inception -- I'm sorry, let me strike that.
THE COURT: I think yesterday the evidence was that buffers and caches were relatively the same thing.
MR. GAUDET: And Your Honor, that was his point, and

that is the point I intend to impeach; that buffering is a common thing that has to be there in every -- to have a processor; a cache is a specific thing that is different.

THE COURT: What does a buffer do?

MR. GAUDET: Your Honor -- well, is that to me or the witness?

THE COURT: The witness.

THE WITNESS: Oh, sure. A buffer is typically something that, it's a memory that holds something. Often for future use. Typically buffers have some sort of ordering associated with them. So like a first-in/first-out buffer is very common, and in that case, as things arrive they may be held in the buffer, and the first thing that came in would be the first thing that came out. But it's a memory for holding things.

THE COURT: What's a cache?

THE WITNESS: A cache is also often used, is used in the same way as a memory for holding things. They're very similar. And with a cache you don't typically or necessarily have an ordering associated with it. I mean, it can have an ordering, but it doesn't have to. But a cache is typically used as a memory that holds information that you expect to be using in the near future.

THE COURT: Okay.

MR. GAUDET: And Your Honor, that's about as far as we

need to go on that point. We're going to obviously give you some more perspective on it from our own witnesses.

THE COURT: All right.

MR. GAUDET: I'd like to move to admit DTX-1650.

THE COURT: Is that the Hughes?

MR. GAUDET: It is, Your Honor.

THE COURT: What's the designation?

MR. GAUDET: Your Honor, that's DTX-1650.

THE COURT: DTX-1650. And that's Hughes.

MR. GAUDET: That's Hughes. It's the counter.

THE COURT: 2589.

Well, something is wrong here, because the citation at the bottom contains more information that I'm looking at.

MR. GAUDET: Your Honor, there is a series of objections and lawyer colloquy, and we did our best to remove that rather than burdening Your Honor with that material. So these were the, this was everything in terms of the --

THE COURT: Okay.

MR. GAUDET: -- that's my understanding.

THE COURT: All right. And you want that admitted?

MR. GAUDET: We want this admitted, yes, Your Honor.

THE COURT: All right. That's admitted.

(Exhibit DTX-1650 received in evidence.)

MR. GAUDET: Thank you.

BY MR. GAUDET:

Q. With respect to the --

MR. GAUDET: Let's go back to the claim language, Mr. Simons, if you would.

BY MR. GAUDET:

Q. Dr. Mitzenmacher, in the claim, whatever it is that a cache is, let's leave aside any discussion, any debate about that for a minute, whatever it is that the cache element is in H2, that's got to happen in response to a signal that, to process packets in accordance with the second rule set. And if you look at claim element H, that tells you the signal, and then H2 tells you that you've got to cache something responsive to that signal. My question, is that generally fair?

A. I mean, I think you're just reading the claim elements, but sure, I think I understand that.

MR. GAUDET: And just very briefly Your Honor, there is one snippet of source code that I wanted to raise with the witness, and to do that we would have to ask just very briefly to seal the courtroom.

THE COURT: All right. Is this in the same exhibit that the plaintiff used?

(Confidential Testimony to Page 843, Line 2 redacted and filed under seal.)

* * *

* * *

BY MR. GAUDET:

Q. Dr. Mitzenmacher, let's actually pull up PTX-1291. This is a document you discussed yesterday.

THE COURT: Is that already in evidence?

MR. GAUDET: It is in evidence, Your Honor. It should be in their binder. And we're again --

THE COURT: 1291?

MR. GAUDET: 1291. And we're again going to a Page 007 in this one.

THE COURT: All right.

MR. GAUDET: Give me one second.

BY MR. GAUDET:

Q. Dr. Mitzenmacher, this document relates to the Firepower Management Center, correct?

A. I believe so, yes.

Q. It talks about the various ways that the Firepower Management Center can pull in threat intelligence; is that fair?

A. I think that's one of the things it talks about.

Q. And the Court asked a question of you yesterday and I want to be sure I understand. Threat intelligence arrives at the Firepower Management Center, correct? Or the Threat Intelligence Detector, correct?

A. Yes.

Q. And then the Firepower Management Center uses that

intelligence to create rules; is that correct?

A. So I would say it's getting rules and rule information from it, and it is then constructing a rule set to pass on to the devices. In doing so, it may eliminate some of the rules it received or decide to change them or to include or not include them. But it obtains rules and then optimizes, preprocesses and optimizes them.

Q. A rule has a condition and then an action, right? That's what makes it a rule?

A. Yes.

Q. Your understanding is that the Firepower Management device is receiving things from third parties that have a condition and an action that's required if that condition is satisfied?

A. Yes. That's some of the threat information it receives, yes.

Q. Okay. I just wanted to clarify it.

MR. GAUDET: Your Honor, that's all I have on this patent. We can move on to the last patent, with your permission.

THE COURT: Okay. Now we're moving to the '205 patent?

MR. GAUDET: That's correct, Your Honor.

THE COURT: What did we call this? The dynamic security patent? I think that's what we called it.

THE WITNESS: Yep. Yes, sir.

THE COURT: Okay.

MR. GAUDET: And if we could, Mr. Simons, pull up JTX-1? And I want to go to claim 63. Should be almost at the back of the document.

Your Honor, the good news is I do think this will be the quickest of the three patents.

THE COURT: JTX-1, page -- that's Bates 63? 563, is it?

MR. GAUDET: Your Honor, I referred to it as claim 63. And let me --

THE COURT: Oh, I thought you said page. I'm sorry.

MR. GAUDET: I apologize. Claim 63. And we will have a Bates number for you in just a moment.

Let's blow up claim 63. I'm sorry, Your Honor, it's Bates number 538 within JTX-1.

THE WITNESS: I just want to state I have a copy of that in my binder, so if I look the other way I'm looking at a paper copy.

MR. GAUDET: Terrific.

THE COURT: Okay.

MR. GAUDET: Let's blow up claim 63, Mr. Simons.

BY MR. GAUDET:

Q. Now, Dr. Mitzenmacher, the '205 patent and claim 63, it claims a specific type of a rule; is that generally fair?

A. I mean it talks about at least one rule specifying. Is

that what you're referring to, or...

Q. Yeah. And I'm sorry, let me be more specific. Let's highlight the Receive element. Just highlight in yellow the entire Receive element.

You see towards the end of the second line there's a reference to "at least one rule specifying." Do you see that?

A. Yes.

Q. Okay. And it's got a specific -- a set of network addresses, correct?

A. Yes.

Q. And this rule also has to specify a Session Initiation Protocol, SIP, Uniform Resource Identifier, URI, correct?

A. So again, I think this has, I think, come up before, so I think you're reading it differently. It says that there's a comprising at least one rule specifying a set of network addresses and a Session Initiation Protocol, Uniform Resource Identifier. So my understanding that at least one rule is specifying those things, it doesn't have to be one rule specifying those things, because otherwise it would just say one rule.

Q. Okay. Can we agree at least one rule has to specify a Session Initiation Protocol, SIP, Uniform Resource Identifier, URI?

A. Yes. That's part of it, I think.

Q. And I want to, again, to orient ourselves, where does

this -- where are you saying this rule lives? What device, what Cisco device has this rule?

A. So in the cases this would be sort of the end devices, the routers and switches or the firewalls.

Q. I want to talk a little bit more about that long phrase, Session Initiation Protocol, SIP, Uniform Resource Identifier, URI. Do you see that?

A. Yes.

Q. Okay. And you talked a little bit on direct about something called Voice Over Internet Protocol, Voice Over IP. So that's using the Internet to make telephone calls, correct?

A. Yes.

Q. And so it's sort of you're using the Internet as a way of getting calls around the world using, as opposed to using the telephone company and their wires; is that generally fair?

A. I mean, I think that's at least part of the intention of Voice Over IP is to allow that and other functionalities as well.

Q. And this Voice Over IP way of making telephone calls, that's been around for a couple of decades; is that fair?

A. You know, I'd have to look up when it started. It's been around at least a while.

Q. Okay. And the Session Initiation Protocol, SIP, Uniform Resource Identifier, URI, that's sort of like the function of a telephone number; is that generally fair?

A. It certainly can be. It's, you know, it's an identification or way of identifying, I guess, a resource. You know, if it gets -- I think it's broader than just a telephone number, but one of the roles it could play is sort of an equivalent or like a version of like a telephone number in this sort of system.

Q. Okay. And there's an Internet standard that actually defines what a Session Initiation Protocol, SIP, Uniform Resource Identifier, URI, is that standard is -- I'm sorry, go ahead.

A. Yeah. There are standards that talk about these things.

Q. And that's Standard Request for Comment or RFC 3261. Does that sound familiar?

A. Yeah, I think so.

Q. Okay. Let's pull up DTX-1296.

THE COURT: Did you say PTX?

MR. GAUDET: Your Honor, Defendant's. DTX. And this should be in the small cross-examination binder, Your Honor.

THE COURT: DTX.

MR. GAUDET: DTX.

THE COURT: 1296. Is this already in evidence or not?

MR. GAUDET: It is not in evidence and I will move it into evidence.

THE COURT: This is the SIP. And you're moving that into evidence?

MR. GAUDET: Yes, Your Honor. We move Defendant's Exhibit 1296 into evidence.

THE COURT: That will be admitted.

(Exhibit DTX-1296 received in evidence.)

BY MR. GAUDET:

Q. Dr. Mitzenmacher, are you familiar with the document that's marked Plaintiff's -- I'm sorry, Defendant's Exhibit 1296?

A. I believe I've seen this before and I think I probably referenced it in my report.

Q. Okay. And the title there, SIP Session Initiation Protocol, do you see that?

A. Yes.

Q. And that's the same SIP Session Initiation Protocol that's referenced in the claim?

A. That's my understanding.

Q. Okay. And this is one of these Internet standards that allows everybody to be systems that can communicate and get along and interoperate. Is that generally fair?

A. Yeah. I mean, I think this might have been talked about in the tutorials. You know, there are working groups that train, create rules, which is one of the documents from those groups.

Q. And let's turn to Page 148 of the document.

MR. GAUDET: Which, Your Honor, should be the second page in your binder.

THE COURT: Okay.

BY MR. GAUDET:

Q. And Dr. Mitzenmacher, you see the top of the page says SIP and Uniform Resource Identifiers?

A. Yes.

Q. And the SIP, that's the Session Initiation Protocol in the claim language, correct?

A. Yes.

Q. And the Uniform Resource Indicator, is that the same thing as the Uniform Resource Indicator, URI, in the claim? Is that fair?

A. Yeah. It is sort of odd. I hadn't noticed this before about the sort of cross language here. In the title it uses Indicator, in the patent it uses Identifier. I typically think of the "I" there as being Identifier. But you know, I can't believe there is much of a difference.

Q. I was going to say, you're comfortable that they're referring to the same thing; is that fair?

A. I believe they're likely meant to be referring to the same sort of thing.

Q. Let's -- about halfway down the page there's something that says SIP and SIPS URI components. Do you see that?

A. Yes.

MR. GAUDET: Let's highlight that, Mr. Simons.

THE COURT: What are we looking at now?

MR. GAUDET: I wanted to call your attention to the

first sentence that says the SIP and SIPS schemes follow the guidelines in RFC 2396. We can highlight that sentence.

BY MR. GAUDET:

Q. See that?

A. Yes.

Q. What is a SIP scheme?

A. I believe it's -- you know, I mean it's just saying that when you are following the Session Initiation Protocol, or the SIPS is the secure version that I believe uses TLS -- sorry, another acronym. That uses additional security on top of the Session Initiation Protocol.

Q. Okay. And then after that paragraph there's an example that starts with the word SIP. Do you see that?

A. Yes.

Q. It's really the form, right, of an example. It starts with SIP colon. Do you see that?

A. Yes.

Q. So likewise a Session Initiation Protocol, SIP, Uniform Resource Identifier, URI, address it starts with that SIP colon scheme, correct?

A. I mean, in this example or this formatting, you know, generally in such situations it may be implicit or understood.

Q. Okay. Sir, the -- now turning back to the accused products, a Session Initiation Protocol, SIP, Uniform Resource Identifier, URI, that doesn't appear in the header of a packet;

is that correct?
A. SIP URI? --
Q. Yeah. That address would not be in the header of a packet; is that fair?
A. I, I think, you know, I think we'd have to get more concrete in the question, since, you know, for instance, the SIP corresponds to a certain port, and that would be in the header of the packet. You know, the hostname can appear in the packet when it's an IP address. So I think it's just an ill-formed question. It would depend on the context.
Q. Okay. And I want to be sure you get the context. The entire address, the entire SIP, Session Initiation Protocol, Uniform Resource Identifier address, would not be contained in the header of a packet; is that fair?
A. Again, I think I'd have to caveat it with the statements I was making. It will depend on what you were referring to, particularly as the address, which can be the IP address, domain and so on. So like I don't think I can completely agree with that.
Q. Okay. Sir, in the course of your direct examination you never showed us a rule on a router or switch that had a Session Initiation Protocol, Uniform Resource Identifier identified in the rule, right?
A. I don't recall my exact testimony, but I think if I would say with the understanding that a SIP URI can be denoted or

correspond to the host as described here, I think I would disagree with that. But I would have to look over my testimony, and I'm pretty sure we had rules that had hosts as IP addresses shown.

Q. Let me try it this way. Would you agree that you never showed a rule in the direct examination that started with a SIP protocol, an actual rule on a router or switch that started with the -- that had an address that started with SIP, that SIP scheme?

A. Again, that may have been put in in other forms or other formats such as the port number. I mean, I don't think it was necessarily formatted that way, like it wrote the letters out, but there were, as I described in both my literal and DOE infringement analyses, rules that corresponded to these SIP URIs.

Q. We talked about some StealthWatch source code, do you recall that?

A. Yes.

Q. Okay. And do you recall that the top of that StealthWatch source code -- let me see if I can do this without asking to seal the courtroom -- but it related to something called the flow sensor. Do you recall that?

A. It may have. I'm not -- I don't remember the code document, but if you say it related to a flow sensor, that would be fine.

Q. It says what it says and we'll have our experts. This is the point I want to confirm with you: A flow sensor, that's a different Cisco product than a Cisco router or a Cisco switch, correct?

A. A flow sensor? I honestly can't recall the entire usage of Cisco's uses of that terminology so I wouldn't want to say without going back and checking. I just can't recall.

Q. You also, sir, you relied on -- let me ask you --

MR. GAUDET: Pull up Plaintiff's Exhibit 1289. We'll go to Bates pages 1911.

THE COURT: Now, 1289, whose exhibit is this?

MR. GAUDET: Your Honor, this was the plaintiff's exhibit that, it should be in the plaintiff's binder, and I believe it was admitted, Your Honor.

COURTROOM DEPUTY CLERK: Yes.

THE COURT: 1289. And what page?

MR. GAUDET: Page 1911, Your Honor.

THE COURT: Can you give me the Bates number of that?

MR. GAUDET: Your Honor, the Bates number is 1911 -- I'm sorry, so 6310.1911. So it should end in 1911, Your Honor.

THE COURT: All right. I've got a 1912. I don't have a 1911.

MR. GAUDET: Let's go to 1912. That's fine.

BY MR. GAUDET:

Q. So Dr. Mitzenmacher, do you see Page 1912 here?

A. Yes.
Q. Okay. And this is -- this was the page that you rely on in your direct examination as evidence that a Cisco firewall could satisfy the claim element relating to the Session Initiation Protocol, Uniform Resource Identifier? Do you recall that?
A. I mean, I think I was using this to say this is some of the information that is examined and looked at and pulled out in the preprocessor for later rules. One of the things it looks at is the URI.
Q. Okay. And what I want to do now is set this side-by-side with Defendant's Exhibit 837.
MR. GAUDET: And Your Honor, this is one of those moments that we did the best we could to predict things, but this came up during the direct examination, so we emailed a copy during the break. You don't have this document in your binder.
BY MR. GAUDET:
Q. Dr. Mitzenmacher, you see trial exhibit references Sourcefire's 3D6 system. Do you see that?
A. Yes.
Q. Sourcefire's 3D system, that was a Sourcefire system dealing with security, correct?
A. I can't recall that I've opined on, for instance, this specific system. You know, you can state that. I don't recall if I examined this system. It doesn't like it. It looked like this might have been studied on the validity side, which I

wasn't studying.

Q. Are you generally familiar with Sourcefire?

A. I am aware of Sourcefire as a company as it relates to this case.

Q. Okay. And Cisco bought Sourcefire in 2013?

A. That is, I think -- I'd have to check the date, but that's again how I understand Sourcefire relates to the case.

Q. Okay. Let's go to Page 2 of this document. And you see --

THE COURT: Page?

MR. GAUDET: The second page, Your Honor.

THE COURT: Which would be Bates 589?

MR. GAUDET: It should be Bates 002, Your Honor.

Your Honor, I've been informed that there was a problem and that Page 2 did not make it to you. I'm just going to ask one question on this one and then we'll move to the page that you do have, which is:

BY MR. GAUDET:

Q. Just for context, do you see at the very bottom of this page it references a November, 2011 --

THE COURT: Can you blow that up? I can't read it.

MR. GAUDET: Let's below that up.

MR. HANNAH: And Your Honor, we would just like to object on foundational grounds. The witness just said that he hasn't seen or opined on this document, so it appears that counsel's just going to be testifying about this document since

the witness can't talk about it.

THE COURT: We can look at the language on the document, see what it says.

MR. GAUDET: That's all I'm going to do, Your Honor.

THE COURT: You're going to have to blow it up.

MR. GAUDET: Yes. So blow up that, and...

BY MR. GAUDET:

Q. Dr. Mitzenmacher, my question --

THE COURT: All that is is a date.

MR. GAUDET: That's it.

BY MR. GAUDET:

Q. On the face of this document it at least appears that it was published in November of 2011. Is that at least what the face of the document would suggest?

A. I'm sorry, what that a question? That sounded like a statement.

BY MR. GAUDET:

Q. Simply, the face of the document states November 10 -- sorry, November 1st, 2011. That's the only question.

A. I see the text that you blew up.

Q. Now let's turn to Page 589 of this document. And what I want to do is highlight on the left in blue from "decoding" down to about just before "SIP preprocessor options".

MR. GAUDET: Give us just one minute.

Don't blow it up, highlight it.

I apologize, Your honor. We're working out the kinks.

And then on the left side here -- so the right side from "decoding". The first bullet down through the second-to-last bullet. SIP Rule Keywords.

BY MR. GAUDET:

Q. And my question here, Dr. Mitzenmacher, is just to confirm that the language that you relied on is literally verbatim the language that appears in a document from Sourcefire on the right?

A. So I mean, I think there are some changes between the two, but I would certainly I also note that there's similar language.

Q. You mean the formatting is different, sir?

A. Like in the bullets below, I notice some extra words and page numbers and other things like -- I'm just saying they're not exactly the same, but I agree with you, that there's similar language in both.

Q. That's plenty.

And then with respect to --

THE COURT: Now, wait.

MR. GAUDET: I'm sorry, Your Honor?

(Pause in the record.)

THE COURT: Well, they're not the same, that's for sure.

THE WITNESS: That's what I said. They're not the same, but they have similar, some similar language.

THE COURT: Well, they're not the same.

MR. GAUDET: Your Honor, the formatting is different, and I think --

THE COURT: No --

MR. GAUDET: -- there's an extra.

THE COURT: -- no, it's more different than the formatting. There's just more volume --

MR. GAUDET: On the older one.

THE COURT: -- on the right than there is on the left.

MR. GAUDET: Yeah. And let me ask a better question.

BY MR. GAUDET:

Q. All the words in the newer one, all those words in the newer one were included in the older one. That's really the point.

A. I mean, do you want me to do the exercise of doing a check? Like, I mean, it's on the screen. If you really want me to do a word-by-word check I can try and take a few minutes. But again, I haven't seen this other document before so, you know...

Q. That's fine.

THE COURT: I can tell you that they're not the same. The formatting's different and the words are different.

MR. GAUDET: Your Honor, our point is that the one on the right, the older document, includes all of the words from the one on the left. There's an extra sentence or two in the highlighted portions, but unless we've missed it, I apologize,

but all of these words on the left appear in the older document on the right. That was the point.

THE COURT: Well, that may be, but --

MR. GAUDET: That was it.

THE COURT: -- they're not the same.

MR. GAUDET: There are more words than the one on the right. That's obvious.

MR. GAUDET: Right.

THE COURT: I don't know what effect the more words have on the meaning of the two. Maybe the witness can tell us if it does or doesn't.

BY MR. GAUDET:

Q. And Dr. Mitzenmacher, do you have any comment on the additional words?

A. I mean, I haven't looked. Like I say, I haven't seen this document before. I haven't studied it. I suppose you're going to have witnesses that can talk about it if -- but you know --

MR. GAUDET: Your Honor, again, this is just one of those moments where -- I'm sorry.

THE WITNESS: I don't think it affects my analysis, if that's what you're asking.

MR. GAUDET: That's it. We were simply laying a foundation with this witness, and we're going to bring it together when it's our turn to put our case on. That's as far as we're going to go with this, Your Honor.

THE COURT: Well, the witness says he doesn't think it affects his analysis, so...

MR. GAUDET: Last point on this patent --

THE COURT: Well, this new thing is not going to be admitted until it's identified.

MR. GAUDET: Yes, Your Honor.

THE COURT: Exhibit 837, DTX-837 is not admitted at this time.

MR. GAUDET: Yes.

BY MR. GAUDET:

Q. Now, the other issue that we talked about -- let me strike that, actually.

Let's pull back up the claim language if we could.

This is claim 63 of the '205 patent we were looking at earlier. I can probably start without having the claim language up. You recall talking about encapsulation, right, Dr. Mitzenmacher?

A. Yes.

Q. And you referred to that as sort of a detour where a packet arrives, it gets encapsulated and then it gets rerouted?

A. Yes.

Q. Okay. And now, sir, on direct examination did you identify a rule that has, as the condition, the presence of a Session Initiation Protocol, SIP, Uniform Resource Identifier, as the condition, and the result being if it's got that SIP URI

address, then it will encapsulate the packet. Did you show us a rule that actually did all this?

A. I mean, I don't think the claim language calls for a specific rule to encapsulate. I realize there's some -- I think that has come up before. I don't think that the claim language specifically calls for that. I can't recall that I would have shown something like that in my testimony. I don't think I focused on that point. But you know, given the rule potential for routing, I think that there are cases where it would have that potential, yes.

Q. Okay. Encapsulation, the idea of encapsulating packets, that's not something Centripetal invented, right? That basic concept has been around for a long time?

A. At a high level, I believe that concept existed prior to Centripetal.

Q. Okay. And you'll also agree with me, sir, that the possibility that there could be a rule that identifies a Session Initiation Protocol, SIP, Uniform Resource Identifier, URI, and that same packet also gets encapsulated, that mere possibility is not enough to satisfy the claim. The claim requires that there actually be such a rule that satisfies those elements?

A. My understanding is this is a system claim, so it would have the code to do all these things. It would have a code for rules and the code for the encapsulations and so on as I've described. So I guess I'm not quite clear on your question. I

think sort of the requirements you're asking about sound more like a method claim issue to me, but... that's a legal question.

My understanding is it has the code, it has the functionality to do all these things.

Q. And your point is the system doesn't have to be actually configured with the rule? Is that your point?

A. No. My point is like the system is configured to do all these actions, right? You know, someone may have to set up a rule to do it, but the system has the code to do all this, right? It's configured to do this.

Q. You haven't shown us any examples of where someone actually set up a rule to do this, right?

A. Set up an example? I don't recall specifically showing that. But again, what I was showing was the code, the functionality, the system that's set up to do that. Again, I think of the -- you know, showing things like that is what I've -- corresponds to like a method claim analysis.

Q. I've got one more question. And this is going back on the 806 patent, so I guess I'm treading back, but I think it's really one question.

Of course those are famous last words. Maybe the least-credible things lawyers ever say.

On the '806 patent, that's the rule-swapping patent, right?

A. Okay. Is that the question?

No, just...

Q. I'm done.

(Inaudible.)

Q. In the accused products, packets are buffered as part of packet processing and filtering even when rules are not being swapped, right?

A. There may be multiple reasons why you put a packet in a buffer or keep a packet in a buffer. Of course here we're talking about, in the patent you're talking about having a packet in the cache because it's not ready to process precisely because you're doing the rule swap, and that's what I was focused on. There may be other things going on in the system. I'm focused on the claim, and the claim talks about caching because you're swapping the rules, as we've discussed. And that's what's going on.

MR. GAUDET: That's everything I have.

THE COURT: All right.

MR. HANNAH: May I proceed, Your Honor?

THE COURT: I was afraid you were going to say that. I hope you'll proceed very rapidly.

MR. HANNAH: All right. Thank you, Your Honor. And I just want to clarify some of the confusing points that came up during the examination.

MR. HANNAH: So we could go backwards or we could start with the '193, we can start with the '205. I don't know what Your Honor prefers in terms of your notes.

THE COURT: Doesn't make any deference.

MR. HANNAH: All right. Let's start with the '205 then since it's fresh in our minds.

REDIRECT EXAMINATION

BY MR. HANNAH:

Q. Doctor, if we would go to JTX-1, if we go to column 14 of the document, that ends in Bates No. 530. Column 14.

THE COURT: 530, column 14.

MR. HANNAH: Yes.

BY MR. HANNAH:

Q. Doctor, you remember on your examination counsel was asking you questions regarding the SIP URI?

A. Yes.

Q. And he was asking you questions as to whether the SIP portion actually had to be within the SIP URI. Do you remember that?

A. Yes.

Q. So if we look at column 14, and starting at the top going to about line 10, can you explain for the Court how this informs your opinion as to whether the actual letters SIP have to be in the rule or if it can just be the domain name?

A. I mean, the patent discusses SIP URI, and I think it uses this example like exampleuser@exampledomain.com and there is no SIP, S-I-P, colon. That's because, again, I think it's understood. That's the scheme or the protocol. There may be

many contexts where you don't need those actual letters to be able to understand if you're blocking things related to that SIP URI.

Q. And just to be clear, the accused routers and switches, they use the domain name as part of the header in performing their analysis for the SIP traffic; is that right?

A. That's part of what they look at, yes.

Q. All right. Doctor, I'd like to turn your attention to the '806 patent. And for the '806 patent, counsel showed you the deposition testimony of Martin Hughes, which was DTX-1650.

MR. HANNAH: Can we put that up, please?

BY MR. HANNAH:

Q. Now Doctor, I'm not sure that this got driven home or not, but when you read the last question and answer, does this inform your opinion as to whether the Cisco employees themselves equate caches and packet buffers?

A. Yeah. I mean, so I guess -- so he was asked a question about storing a packet in a cache, and he himself, you know, says oh, yeah, that's put in a packet buffer where packets are stored before processing. So he connects or understands caches and buffers are sort of, you know, used to refer to sort of memory to hold items.

Q. Doctor, during your testimony again with -- your cross-examination with regard to the '806 patent, there was some notion from counsel that there's no delay in the new system

between swapping rules. Do you remember him talking about this delay aspect?

A. Yeah.

Q. So if we go to PTX-1196 which was shown to you on direct examination, I'd like just to remind you and show you Page 7 of this document, and in particular the last line.

THE COURT: Wait a minute. This is PTX...

MR. HANNAH: 1196.

THE COURT: 1196 at Page 007?

MR. HANNAH: Yes, Your Honor.

THE COURT: All right. What's the language you're referring to here?

MR. HANNAH: So the last line of 1.4 where it says "Customer Needs", it specifically says that "As long as the whole update transaction is atomic; i.e. no gap between removal of old rules and addition of new rules, it is acceptable to have a reasonable amount of delay for the new rules to take effect."

Doctor, can you please explain how this informs your opinion as to whether there is an amount of delay in the new systems that are accused of infringement between when the old rules take effect -- I mean between when the new rules take effect versus the old rules?

A. Yeah. I mean, like I said, there has to be some delay. There's a switchover, and we talked about that. With regard to the code, you know, you have to actually do the switch, validate

that the switch took effect and signal that the switch took effect and then start up the processing again. So there's certainly going to be some delay, right? And the issue is, really is just is it a -- obviously whenever there's a delay in a system you'd like to minimize it. And as it says here, is it acceptable? The question you have to ask in design is, is it acceptable to have that delay. And here, you know, as it says, it is acceptable to have a reasonable amount of delay for the rules to take effect. Particularly when the other option is to run the risk, as discussed earlier in here, of having dropped or dropped packets, packets that are dropped because they couldn't be handled because the system was overloaded.

Q. And you anticipated my next question, is that the old system tried to eliminate the delay, but this new system introduces some delay between the old rule set and the new rule set; is that right?

A. It has this acceptable amount of delay, right, but it does that by doing a different sort of structure precisely to avoid the problems in the old system.

Q. Thank you, Doctor.

Now let's turn to the '193 patent. And the 193 patent, I want to look at the claims. We can look at claim 18, but it has the same corresponding limitation in claim 19. And if we look at the responsive -- we can just blow the "responsive to", the first "responsive to".

Now, there was some discussion, and I have to admit it was a bit confusing in terms of this element, and I just want to ask you to clarify for the record, how do the switches and routers prevent a particular type of data transfer using the header information?

A. In particular I was talking about preventing exfiltration, and the exfiltration is based on a certain host. And so you would -- the primary goal of the quarantine is to block that host from accessing certain other networks. And it does that through the header information. It can block. It looks at the person trying to reach out from inside and it blocks to where they can go to. So that's based on the header information.

Q. And if we look at PTX-1262, which you referred to in your direct testimony, and if we look at the page ending in Bates number 999.

THE COURT: Just a minute. Where are you now?

MR. HANNAH: PTX-1262, and in particular on page, it's 77 of the document, but Page 999 is the Bates number.

THE COURT: All right.

BY MR. HANNAH:

Q. If we look at "Policy And ACL", and Doctor, do you remember testifying about this in your direct testimony with regard to the '193 patent?

A. Yes.

Q. And if we look at the second line and highlight that whole

thing, it starts with TCAM matching?
A. Yes.
Q. So can you explain how this informs your opinion that a particular type of data transfer can be prevented using the header information?
A. Sure. So you're trying to prevent a type of data flow from, potentially from one location to another location or in particular, from potentially several locations out to another location. And that's handled by a combination of information such as the IPv4 addresses. You look at the addresses of the people who are trying to communicate, and in particular, as we talked about, that SGT, the Scalable Group Tag, right. So that group tag is what says, hey, this is actually a host that's been quarantined. So you don't even have to say I'm going to restrict this host, although that will be the action. You say I can restrict these collections of hosts from reaching the outside world because they all have this Scalable Group Tag.
Q. And just to be clear, you can look at this information not in the payload but in the header as well, correct?
A. Yes. This is additional information. It's not just the information we were talking about.
Q. And finally, Doctor, you were asked a number of questions about certain actions that had to be performed in order to meet limitations. Can you explain the types of claims that we have in this case, the system and computer-readable media and what's

required in order to infringe?

A. Right. So you know, system claims in particular, you have to have a system that has the functionality to perform the operations. And all of these systems have that functionality. The functionality is embedded in the code, right, in the code that runs on the hardware, that runs these machines. And that's also why it satisfies the computer-readable media claims. I mean all of this is, you know, the software that runs on these machines, these instructions that tell the machines to carry out these processes, and all of them, all of these components have the code that allow them to do these steps.

MR. HANNAH: All right. Thank you, Doctor.

Your Honor, I have no further questions.

THE COURT: All right. Is there any --

MR. GAUDET: Your Honor, there are a few points we might want to explore, but I think it makes sense for all involved for us to do it with our own witnesses.

THE COURT: What?

MR. GAUDET: I'm sorry, I thought you were asking if I had any recross.

THE COURT: I am.

MR. GAUDET: The short answer is no. There is some points that I may have wanted to explore, but I think it makes sense for us simply to do them with our own witnesses.

THE COURT: All right. Will this witness -- can he be

released or is he going to be recalled or what?

MR. HANNAH: He can be released, Your Honor. We're not going to recall him.

THE COURT: All right. Doctor, you're excused as a witness. And what that means is that you cannot discuss your testimony with any other witness in the case until the case is concluded. But you may, if you wish, observe the case on audio if you have any interest in doing so.

THE WITNESS: All right. Thank you, sir.

THE COURT: But other than that, you're excused.

THE WITNESS: Thank you, sir. Thank you everyone.

MR. GAUDET: Thank you, Dr. Mitzenmacher.

THE COURT: Are you ready with the next witness?

MR. ANDRE: We are, Your Honor. Paul Andre for plaintiff Centripetal. I just had to switch out my name on the camera there. And we're calling Dr. Eric Cole to the stand.

THE COURT: Dr. Harry...

MR. ANDRE: Eric Cole. E-r-i-c, C-o-l-e.

THE COURT: Eric?

MR. ANDRE: Yes. Eric Cole.

THE COURT: C-o-l-e?

MR. ANDRE: Yes.

THE COURT: Where are you, Dr. Cole?

THE WITNESS: I am in my home office. I have a studio here because we do a lot of podcasts and interviews and training

classes.

THE COURT: I mean geographically.

THE WITNESS: Oh, sorry. Ashburn, Virginia.

THE COURT: Where in Virginia?

THE WITNESS: Ashburn. Right near Dulles Airport.

THE COURT: Ashburn. Okay.

You may proceed, Mr. Andre.

MR. ANDRE: Thank Your Honor.

ERIC COLE, having been duly sworn, was examined and testified as follows:

DIRECT EXAMINATION

BY MR. HANNAH:

Q. Good afternoon, Dr. Cole.

A. Good afternoon.

Q. Thank you for waiting patiently for us to get to you.

THE WITNESS: My pleasure.

THE COURT: Let me collect a new set of books here.

(Pause in the record.)

THE COURT: All right. You may proceed.

MR. ANDRE: Thank Your Honor.

BY MR. ANDRE:

Q. Dr. Cole, let's start out with talking about your qualifications. Can you tell us -- and there's a slide for this -- could you tell us about your education?

A. I have a Bachelor's and Master's degree in computer science

from New York Institute of Technology. I have my Doctorate from Pace University, in which my dissertation was focused on cybersecurity, data protection and data leakage.

Q. And could you tell us about some of your certifications in cybersecurity?

A. Yes. In cybersecurity there is two main certifications. The first one is Certified Information Systems Security Professional, and that's sometimes abbreviated -- I know we have a ton of acronyms in this case -- CISSP. And that I earned in the mid '90s and was one of the first few hundred people to have my CISSP, and I still maintain that certification today.

The second main certification in cybersecurity is the Global Security Essential Certification, known as GSEC. And that certification I do not actually hold, because I created the certification and wrote the test questions. So it would be a conflict of interest for me to actually take that exam.

Q. I noticed that you were a Commissioner of cybersecurity for the 44th President. Have you worked for the White House and other Presidents as well, and what did you do for the White House?

A. Yes. So I've advised the last three Presidents of the United States on cybersecurity. It was the previous President actually formed a commission, so I was one of the Commissioners, or I was one of the authors of the guide for protecting cyberspace. I was also involved in securing the President's

Blackberry when that rolled out, and also for securing and protecting his social media accounts.

Q. Let's start with -- go to the next slide -- and talk about some of your employment. I see you started your career at the Central Intelligence Agency from 1991 to 1996. Could you tell us, what did you do for the CIA?

A. For the CIA I focused in several different areas. I started off as a artificial intelligence programmer where I actually built expert witness tracking systems that would help the government track, find, terrorists across the world. I then, from that programming experience in artificial intelligence, I then moved into cybersecurity where I was a professional hacker for eight years focusing in on identifying vulnerabilities, flaws and exposures and breaking into various systems around the world.

Q. And I notice you were at the CIA kind of right when the, a little bit from the Internet was taking off and became popular in the mid '90s until a little bit after. Did your training at the CIA, did it involve trying to break -- how the Internet was working and how it would be vulnerable to security attacks?

A. Absolutely. As you mentioned, in the early '90s this was before the World Wide Web existed. We had early connections. So we were one the key testers in a lot of the various protocols, and I was involved in many different working groups in terms of the different protocols we've heard about, Transport

Control Protocol, TCP, and Internet Protocol, IP. I was on many of those different working groups helping to influence, protect and secure those protocols.

Q. And did you get any awards when you were at the CIA or any commendations?

A. Yes, I was received many awards. Multiple awards from the DCI, the director rate of Central Intelligence. I received one of those for actually building and testing some various security protocols. I received a second one for actually helping catch one of the most wanted terrorists in the world. And then a third one for building some internal communication systems.

Q. I won't go through all your employment, but I want to address a few of them. I see from 1999 to present you have been at the SANS Institute, Director of Cyber Defense and Senior Fellow. What does that entail?

A. SANS is another acronym. That stands for System Administration and Network Security. And they're one of the most common, most popular training courses -- sorry, training companies in the world. They give courses all around the world in various locations. And I joined them when they were relatively small and they were running one- or two-day conferences. I was responsible for their cyber defense curriculum.

When I left the CIA, I switched from offense to defense, because what I realized is offense is easy. It's easy to break

into systems. There's always vulnerabilities, there's always flaws. And to be honest with you, I got a little bored. So I switched to defense which is a much harder problem to protect and secure critical systems. So at SANS I was responsible for their cyber defense curriculum where I wrote four of their most popular courses, including Security Essentials, which is their No. 1-selling course, and that has sold to over 50,000 people and I've personally, in a classroom environment, have taught over 25,000, and in virtual environments, an additional 30,000.

Q. And if we go down a little further I see you were the chief scientist at Lockheed-Martin. What did you do for Lockheed-Martin and how did you get there?

A. I got at Lockheed-Martin because they acquired one of the companies that I started. We started a company called The Sytex Group, Inc, which is sometimes referred to as TSGI. And in that group, I was responsible for their intellectual property and doing research and development in new areas of cybersecurity. And based on several of the contracts that we had and some of the advanced research that we were doing, Lockheed-Martin actually decided to acquire us. Typically when a company like Lockheed acquires a government contractor, it's usually because they want the contracts, and they tend to, unfortunately, lay off a lot of people. But based on my expertise in cybersecurity, the current CEO and President, Bob Stevens at the time, kept me on as his chief scientist. So I was responsible

for responding to any breach, any issues or any problems with cybersecurity across all of Lockheed-Martin.

Q. And did you -- was that involving the defense industry?

A. Yes. The defense industry. So I don't know if you recall when there was the hack against the Joint Strike Fighter from foreign countries. I still remember I got the call at 2 a.m. on a Saturday morning, and I was on an airplane at 3:30 flying to Texas to help resolve and minimize the damage and exposure from that attack.

Q. And the last one I want to talk about is McAfee. You're the senior vice-president and chief technology officer. Can you tell us about your time at McAfee?

A. Yes. I was recruited by McAfee around the 2009 time period because that was a interesting transition time in cybersecurity where a lot of the traditional measures were not really working very well and they were losing market share. So they brought me in to head up their technology division, and I worked very closely with customers, analyzing different technology, and eventually rebuilt and revamped their entire product line. And I was also actively involved in not only licensing our technology, but also licensing third-party technology and acquiring and bringing in third-party companies to help augment our security product offering.

Q. Last bullet point there says you worked eight years in the government from various departments: The CIA, the Department of

Defense, FBI, et cetera. Do you hold top-secret clearances?
A. Yes. I believe, if I'm counting correctly, I'm up to five right now. I have a CIA clearance; a Department of Defense clearance, a National Security Agency, NSA, clearance; a Department of Energy Clearance; and an NRC, Nuclear Regulatory Commission clearance.

And just on a side note, several years ago when NRC started moving more to cyber and they needed to go in and do cyber evaluations of all the computers at nuclear power plants, I was actually one of the authors of the cyber regulation for the NRC, which is what all of the inspectors are using today to make sure those critical digital assets at nuclear power plants are properly secure and properly protected.

Q. If we go to the next slide, I just want to talk very briefly about some of the books you've written.

The book on the far left is the *Network Security Bible*. Who uses that book?

A. That's a book that's used wide-range across the industry. I know a lot of colleges use it in their cybersecurity courses. I know a lot of companies have bought anywhere from 30 to 500 copies for their entire staff. And it's also utilized in a lot of different third-party programs.

Q. On top of that book it says -- I'm reading it here, my eyes are not that good -- "compliment your Cisco Academy course instructions." Is it used, is it part of the Cisco training as

well?
A. Yes. Cisco has a publication division called Cisco Press, and they have various certifications. And as part of those certifications in different areas, including network security, they have third-party reference books that they utilize. And my book is one of those reference books that they utilize for their academy.
Q. Now, are all your books geared towards cyber professionals or do you have some books for the laypeople and kids?
A. My original focus was on technology. So you'll notice my first book was *Hackers Beware*. Then we have *Network Security Bible* 1st and 2nd Edition, *Advanced Persistent Threat, Insider threat*, but what I realized several years ago is the problem isn't necessarily the technical people don't know the technology, it's that the average, the doctors, the lawyers, the teachers, the parents, they don't understand that they're a target and that cyber security is their responsibility. So I started writing books to help protect families and parents online, which the main book being *Online Danger*.
MR. ANDRE: Your Honor, at this point we'd like to tender Dr. Cole as an expert in cybersecurity and the cybersecurity industry.
THE COURT: Any voir dire from counsel for the defense?
Mr. Jameson, I see your picture. Is there any voir

dire?

MR. JAMESON: I was on mute, Your Honor.

There is no voir dire and there is no objection to the tender with respect to Dr. Cole offering his expert opinions with respect to infringement.

I would note for the record that we have a *Daubert* motion pending that's Document 247, and that *Daubert* motion deals with the fact that we expect that Dr. Cole is actually going to be offering opinions in the form of expert opinions on the issue of whether or not Cisco copied technology from Centripetal, and we believe that that is a factual issue that has nothing to do with expert credentials. And so we would just like to note for the record that that *Daubert* motion is pending and we do not believe that that's an area for expert testimony.

THE COURT: Well, we'll -- if the proponent of the witness gets into that area, we'll deal with your motion at that time.

MR. JAMESON: Thank you, Your Honor.

THE COURT: And we accept the qualifications of Dr. Cole to testify in the specified areas as an expert.

MR. ANDRE: Thank you, Your Honor.

BY MR. ANDRE:

Q. Dr. Cole, what was your assignment in this case?

A. My assignment in this case was to review Cisco's public documents, confidential documents, engineer's deposition, source

code, and actually test the products, and then determine if the defendant's products infringed two of the patents that, in this case, we are calling the '856 patent and the '176 patent.

Q. Before we get into it, the '856 patent first, when I talk about cybersecurity, what do you mean, how do you understand that term to be applied?

A. Cybersecurity, as you can imagine, is a very broad term. The way that I look at it, it's all about managing risk to your critical assets and critical information. Cybersecurity is all about understanding and mitigating those overall risks. One thing that's important to point out is 100 percent security in any practical sense doesn't exist unless you disconnect from the grid. Because if you have 100 percent security, that's zero functionality. So the way you need to look at it is any time you're adding in functionality, you're decreasing the security. So when you have a system that has a lot of functionality or a lot of capability, it's not going to be 100 percent secure. There is going to be some exposures or issues. So to me, cybersecurity is about prevention is ideal, but detection is a must. You need to recognize that you won't be able to prevent all attacks, and really what you're tying to do with cybersecurity is to contain and control the damage, is to get proper visibility, do proper analysis so you can catch the attack very quickly and contain, minimize and control the overall damage to an organization or an individual.

Q. And I believe you were listening in on Dr. Mitzenmacher's testimony when Judge Morgan asked why is it important to have security at all these different places on routers and switches and firewalls and throughout? Why is layered security important?

A. Layered security, what we sometimes refer to as defense in depth, is based on a simple premise that no single measure is going to be able to protect you. These threats are fairly advanced and fairly sophisticated, and so you need to have as many different layers all working together in order to have a cohesive level of protection.

A great example I like to use is the U.S. military. The U.S. military has multiple branches of the military, and many of those branches have airplanes planes and many of those branches have boats, but if you get more specific, they're different types of airplanes with different branches of the military based on what their mission and focus is. And therefore, even though the United States military and Department of Defense might have some overlap in terms of airplanes, boats and tanks, they're different for different functions, and when you put them all together, they provide a very comprehensive solution to protect the United States. And we do the same thing with cybersecurity. You might have some overlap in some of the different technology, but you really want to have that defense in depth in order to protect, secure and get that visibility so you can contain and

control those threats in a timely manner.

THE COURT: Well, this sounds as if you have to have different policies and rules on different firewalls, switches and routers. That's what we've been talking about, are firewalls, switches and routers. If you've got the same rules on all them, how does that offer you defense in depth?

THE WITNESS: Well, there's a couple ways that works. If you have the same device that has the same rules, the attacker still has to spend effort trying to break into each one, and you're slowing them down in order to get a better chance of catching them. But Your Honor, you're right: In most cases, the effectiveness of these devices really comes in on using the capabilities to be able to build customized rules for each of these different areas and organizations.

For example, I have a bank that I'm responsible for protecting and they have five different devices, and each one has specialized, customized rules on each one. It's the effectiveness of the rules with the technology that allows that bank to have visibility, contain and control the damage.

THE COURT: Okay.

BY MR. ANDRE:

Q. Let's start with the first patent that you're going to be discussing, the '856 patent. Now, what are we calling this patent?

A. We're calling this the encrypted traffic patent.

Q. All right. I'm going to show you what's already been moved into evidence, JTX-5, which is the '856 patent.

MR. ANDRE: And could we pull up Claims 24 and 25?

BY MR. ANDRE:

Q. Could you describe generally speaking what is claim 24 discussing?

THE COURT: Well, 25 is not very legible on the screen?

MR. ANDRE: Well, I'm sorry, yes. It's not on the screen. We'll pull up in a second. The way the screen is put together we can't pull them up at the same time. We're just putting 24 up there now.

THE COURT: All right.

A. So 24 is a system claim, and what that really deals with is being able to detect threats in encrypted traffic without actually decrypting the traffic. So by utilizing information in unencrypted headers and unencrypted packets, you're able to determine if there's any threats within that encrypted traffic without decrypting it. Then you actually can go in and route those packets to a proxy system so proper analysis can be done to minimize those network threats to that environment.

Q. If we turn to claim 25, what is that covering?

A. Except for the beginning portion, this is a computer-readable media claim. But as we'll see in a little bit, the rest of the claims are very, very similar, and in many

cases identical to claim 24. So it's really dealing with the same challenge of being able to detect threats in encrypted traffic without decrypting it and then, based on those threats, be able to route that to a proxy system so appropriate action can be taken.

Q. And what was the -- with respect to the '856 patent, what was the summary of your opinions? I believe we have a slide on that.

A. The summary of my opinion is that Cisco's switches and routers, with Cisco's StealthWatch and Cisco's Identity Services Engine, infringe the '856 patent on claims 24 and 25.

Q. Now let's talk about encrypted traffic and exactly why that causes problems to traditional security. Could you describe -- the headers and payloads, how traditional security detected malware or bad traffic?

A. A lot of the focus -- if you go back more than five years ago, a lot of the focus in cybersecurity was really performing advanced analytics on the payload. So you have technologies like firewalls that start looking at the payload. You have Network Intrusion Detection Systems, which is sometimes referred to as a NIDS, N-I-D-S, which is Network Intrusion Detection System. You also have another technology, Network Intrusion Prevention Systems, known as NIPS, and the focus has always been on how could we do more-advanced analytics of the payload? How could we go and look at the payload and find out what the

adversary is doing, how they're working and operating and trying to break into the systems.

Q. What effect does encryption have on those type of systems?

A. As soon as you go in and encrypt the payload, it allows the adversary to go into stealth mode. Essentially they drop below the radar and they're able to sneak in and cause significant damage. Because if your technology, like your Network Intrusion Detection System, your Network Intrusion Prevention System and some of your advanced firewalls requires payload analysis but you can't read the payload, they are going to be ineffective and miss the attack. And this is one of the reasons why you have examples where you have large hotel chains that had 500 million records compromised. They didn't detect the attack for over years, and the reason is because all their technology was looking at the payload, the attacker was encrypting the payload and therefore the technology was not capable of catching or finding the attack.

Q. And in this case we're going to be talking about Cisco's Encrypted Traffic Analytics; is that correct?

A. That is correct. Sometimes referred to as ETA, with the acronym standing for Encrypted Traffic Analytics.

Q. Can we go ahead to the next slide?

Is the Encrypted Traffic Analytics technology important to Cisco's systems?

A. Yes. This is critical to their systems because it now

allows them to be able to analyze encrypted traffic without actually decrypting it, which is a huge advancement and a critical component. So now via ETA which is built into the routers and also into the StealthWatch, now all of their technology is able to analyze encrypted traffic without actually decrypting it.

Q. I'd like to show you what's been marked as PTX-561.

Dr. Cole, do you recognize this document?

A. Yes, I do. This is a Cisco public document that talks about Encrypted Traffic Analytics with the new, the new Cisco network and StealthWatch.

THE COURT: Let me find that. 561. This is PTX-561. And this is ETA on Cisco's Network and StealthWatch. And you've used those two terms separately.

MR. ANDRE: Your Honor, we'd like to move PTX-561 into evidence.

MR. JAMESON: No objection, Your Honor.

THE COURT: That will be admitted.

(Exhibit PTX-561 received in evidence.)

BY MR. ANDRE:

Q. Dr. Cole, I'd like to focus on that bottom box. This was a document that came out in 2019, how Cisco identified the importance of encrypted traffic at this time period. Could you comment on that, please?

A. Yeah. So they're utilizing a third-party source, Gartner,

which is a highly reliable research organization that many large Fortune 50 companies rely on. So this is a third-party source saying that by 2019, 80 percent of all traffic will be encrypted and 70 percent of network attacks will use encryption. And if you continue to read this document it shows that Cisco understands this problem. This is a growing problem over the last several years, and in order to be able to deal with all this encrypted traffic, especially encrypted traffic being used by adversaries, encrypted traffic analytics became a critical component in being able to identify threats as more and more attackers utilized encrypted communication as a way to try to hide or bypass traditional security measures.

Q. If we turn to the second page of this document ending in Bates number 630, there's a heading called Encrypted Traffic Analytics. If we blow that up first paragraph, and could you describe how that first sentence -- what Cisco's talking about when it talks about Encrypted Traffic Analytics?

A. In my expert opinion, Cisco is recognizing their expertise in network infrastructure and they realized with research that a lot of this technology was becoming less and less effective as more and more attackers encrypted their communication. So they introduced an innovative and revolutionary technology, Encrypted Traffic Analytics, that allows them to be able to analyze encrypted traffic without decrypting it. And the reason why this is so important and they keep emphasizing the without

encryption, is because the old previous way of dealing with encrypted traffic was to actually decrypt it every single time. Well, decrypting traffic is very, very slow. It has a huge security issue, because all of the keys are potentially exposed. And now you could have major privacy issues where you're reading private information that could violate a lot of the cybersecurity regulations. So in order to be able to analyze encrypted traffic without decrypting it was a huge, huge advancement.

Q. If we go down to that same page on the bottom left corner it says the solution elements, and I want to focus on the first two, the Enterprise Switches and the Branch Routers. Do you see that?

A. Yes, I do.

Q. And are these the switches and routers that you'll be giving your opinion on with respect to the '856 patent, the Cisco Catalyst 9000 switching platform and the Cisco ASR 1000 series and 4000 series ISRs and 1000 series?

A. Yes, they are. These are some of the infringing components that I mentioned on the previous slide. And this also informs me that these switches and routers have ETA technology embedded within them.

THE COURT: All right. I want to make a note of these before we move on.

(Pause in the record.)

THE COURT: Okay.

MR. ANDRE: Just one last thing on this document.

BY MR. ANDRE:

Q. In the middle of the page it talks about the Encrypted Traffic Analytics extracts four main data elements, and you see there's four elements listed?

A. Yes, I do.

Q. And we're going to be talking about this a lot, but could you just give an introduction of what we're going to be talking about tomorrow, about what portions of the unencrypted data it uses to detect the encrypted?

A. So as this says, there's four main elements. So the first one is the Sequence of Packet Lengths and Time. So this is going to go in and look at timing conventions, length of the packet, size of the packet. And this is similar to if you're examining packages and you're expecting to get a package that has sneakers but it weighs 60 pounds, that's going to be anomalous into what you're expecting, so it's able to look at parameters in terms of length and time. It then also looks at the initial data packet where it's going to pull information such as Hypertext Transfer Protocol, Universe Resource Locators, domain name, system hostname and addresses. It's also going to look at the byte distribution and then also Transport Layer Security, that's the next version of Secure Socket Layer, SSL, which we've talked about. So it's also going to look at some of

the unique characteristics of the Transport Layer Security handshake and use all of those components that's unencrypted to be able to analyze and identify threats within the encrypted traffic without actually decrypting.

THE COURT: Is that an exhaustive list of what you can look at without de-encrypting?

THE WITNESS: No, Your Honor. These are the four main elements that encrypted traffic analytics extracts and uses, but there actually could be other information in the headers that could also be extracted.

THE COURT: Okay.

MR. ANDRE: Your Honor, I'd like to show what's been marked as PTX-452.

THE COURT: Well, this would be a good time to stop.

MR. ANDRE: Okay.

THE COURT: PTX what?

MR. ANDRE: 452. It was just one -- I was going to talk about the release of this technology.

THE COURT: Okay. Go ahead.

MR. ANDRE: Okay. It will just be a couple minutes, Your Honor.

BY MR. ANDRE:

Q. Dr. Cole, what is this document?

A. This is a document from Cisco that they talk about "Cisco unveils the network of the future that can learn, adapt and

evolve," and they highlight and talk about the importance and criticality of Encrypted Traffic Analytics able to analyze encrypted traffic without actually decrypting it.

Q. What's the date of this document here?

A. June 20th, 2017.

Q. And let's just go down the fifth paragraph in this document. And could you just read that first sentence into the record from the quote from the Cisco executive?

A. Yes, "Cisco's Encrypted Traffic Analytics solves a network security challenge previously thought to be unsolvable."

Q. What does he go on to say there on the ETA uses Cisco's Talos?

A. Yeah. He then goes to talk about the Cyber Threat Intelligence that feeds in. It says "ETA, Encrypted Traffic Analytics, uses Cisco's Talos cyber intelligence to detect known attacks -- my pictures are cutting off -- "of signatures even in encrypted traffic, helping to ensure security while maintaining privacy."

Q. Just in our last minute or two here, was looking at encrypted traffic a problem that people were working on in your industry for several years?

A. Yes. It was a big problem that many people were working on and many people were trying to figure out how to be able to analyze encrypted traffic without decrypting it, because as I mentioned, the old solution of decrypting traffic just wasn't

working.

MR. ANDRE: Your Honor, I'd like to move that exhibit PTX-452, and we may revisit it tomorrow, but now is a good time to take a break.

MR. JAMESON: No objection.

THE COURT: All right.

(Exhibit PTX-452 received in evidence.)

THE COURT: We'll terminate the hearing. I'll ask counsel to remain on.

All right. Is there anything we can take care of at this point that will help move things along tomorrow?

MR. ANDRE: I don't think so, Your Honor. This witness, as you can tell, he's a little different, little faster witness and we'll get through him pretty quickly in the morning, and I think we'll be done with Dr. Cole's testimony in the morning. I imagine the cross-examination will all be done pretty quickly as well, and we'll be very close to getting back on schedule with us dropping the two other witnesses that we talked about earlier. We've also, we're streamlining some of our examinations to make sure we get back on schedule.

THE COURT: Are you intending to go into the copying issue with this witness?

MR. ANDRE: Yes, Your Honor, we will. We're going to lay a foundation of what he's looked at regarding Cisco's communications with Centripetal, the information that

Centripetal gave to Cisco, and then what is the -- based on his expertise in the industry, what is the likelihood that that information was copied. Especially with respect to the Encrypted Traffic Analytics.

THE COURT: All right. Well, I don't think I can pass on whether that comes within the range of expertise without hearing what it is. So I'm not going to try to decide that today.

MR. ANDRE: Your Honor, just -- sorry.

THE COURT: I'll hear it when I hear it.

MR. ANDRE: Your Honor, just one housekeeping matter. We had hoped to get a little further today, but Dr. Nenad Medvidovic will be our next witness. We originally had Jonathan Rogers going, but we had to flip those orders around because Dr. Medvidovic may have some availability issues on Monday, so we just wanted to get those two switched around.

MR. JAMESON: And Your Honor, Woody Jameson. Just want to note for the record that if they still intend to call Mr. Chris Gibbs, he was not disclosed pursuant to the disclosure obligations under the pretrial order. He should have been closed on Monday of this week, he was not, and the first we learned that he might testify was this morning.

THE COURT: What about that?

MR. ANDRE: Your Honor, because of our dropping two witnesses, that moved Mr. Gibbs up. We could put him in on

Monday, that would be fine, if that makes a difference to him.

THE COURT: Well, that may be better.

MR. ANDRE: And he's on our pretrial order as a potential witness to call, so this is not something that should be a --

THE COURT: Well, if he's in the pretrial order, it's just not -- they didn't get the proper notice under the protocol, that's all.

MR. ANDRE: That's fair enough, Your Honor. It was -- when we decided to drop the two witnesses, the two expert witnesses, that took over half a day, probably almost three-fourths of the day out of the calendar, so that moved him up that much faster. We can push him to Monday.

THE COURT: All right. We'll be adjourned until 10 tomorrow.

(Whereupon, proceedings concluded at 4:06 p.m.)

CERTIFICATION

I certify that the foregoing is a true and correct redacted transcript of Volume 6B of the proceedings held in the above-entitled matter.

Paul L. McManus, OCR

Digitally signed by Paul L. McManus, OCR
DN: cn=Paul L. McManus, OCR, c=US, email=pmcmanusocer@verizon.net
Date: 2020.08.10 10:29:17 -04'00'

Paul L. McManus, RMR, FCRR

_____

Date